ORACLE FUSION MIDDLEWARE 11g
IDENTITY MANAGEMENT

Oracle Privileged Account Manager

Disaster Recovery Deployment Considerations

ORACLE WHITE PAPER | AUGUST 2015

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Introduction

The goal of this paper is to provide an overview of the high level design considerations for deploying Oracle Privileged Account Manager (OPAM) in a Disaster Recovery (DR) Environment. This paper walks through a Disaster Recovery scenario to outline what high level steps a failover requires. OPAM is part of the overarching Oracle Identity Governance Suite, but for the purposes of this paper the focus will be on the OPAM component only. This paper is intended to give the reader an understanding of what steps a failover requires, what additional software may be required, what database options should be considered, and other information to help architect an OPAM opportunity. The paper will not discuss implementation details as these will vary widely depending on the customer's environment.

Oracle Privileged Account Manager Overview

Oracle Privileged Account Manager manages privileged accounts that are not being managed by any other Oracle Identity Management components. Accounts are considered "privileged," if they can access sensitive data, can grant access to sensitive data, or can both access and grant access to that data. Privileged accounts are your company's most powerful accounts and they are frequently shared.

For more information on what OPAM is and why it should be used, please reference
http://www.oracle.com/technetwork/middleware/id-mgmt/overview/opam-wp-11gr2-1697093.pdf

When OPAM is deployed within an enterprise, the enterprise may use OPAM to manage a high degree of their privileged accounts via the OPAM password vault and OPAM session manager. Due to the importance of these accounts, it becomes imperative that OPAM can be deployed in a highly available environment and that disaster scenarios can be handled as quickly as possible to ensure these accounts are available to allow the enterprise to continue critical operations.

OPAM is a critical part of the Identity Governance Suite (consisting of Oracle Identity Manager and OPAM) because of the “real time access” it manages for privileged accounts. A prolonged OPAM outage can be more damaging to an organization than an Oracle Identity Manager outage because privileged accounts needed to run the enterprise may not be accessible. Therefore, understanding the Disaster Recovery Failover options for OPAM becomes important in the early implementation stages as a customer calculates the total cost of ownership for the components required to implement a successful Disaster Recovery strategy.

For the purposes of this document, it’s important to understand the basic architecture of a single instance of OPAM.

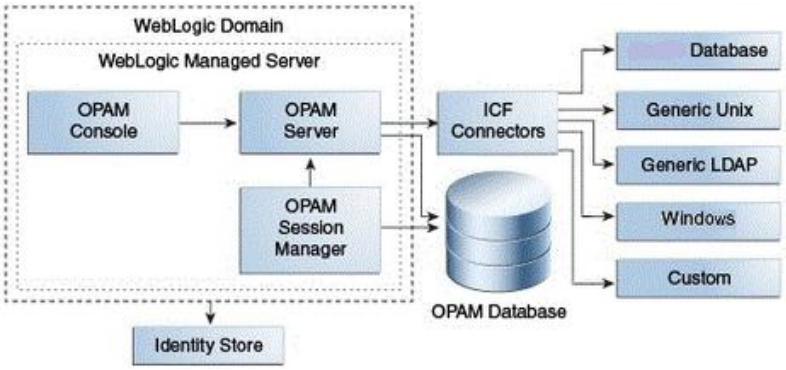

Figure 1: Oracle Privileged Account Manager Single Instance Components

OPAM is deployed in a standard 3 tier architecture. The Web tier (not pictured in Figure 1) acts as a reverse proxy for the OPAM (web-based administration) Console Application. The Application tier runs all of OPAM’s core components within a single WebLogic domain. These components include the OPAM (administration) console, the core OPAM server, and the OPAM session manager. OPAM stores its application data and password vault information in an Oracle database. It is recommended the Oracle DB is encrypted using Advanced Security Option (a restricted license is included with OPAM). The OPAM schema is created in the Oracle database via the Oracle Repository Creation Utility. Oracle Privileged Session Manager relies on the OPAM Database for persistence and communicates with OPAM through its RESTful interfaces. The Oracle Platform Security Services (OPSS) identity

store and the OPSS security store (which includes the Policy Store and credential store) are WebLogic domain-wide constructs, so there is one of each per domain. The OPSS identity store can point to the LDAP directory embedded in WebLogic (out of the box) or to an external LDAP server (not pictured in Figure 1).

For high availability and disaster recovery it is important that the web tier, the application tier (WebLogic), the data tier (Oracle database), and the identity store are scaled appropriately. This paper does not cover detailed sizing guidelines for OPAM. These can be obtained from Product Management. When sizing, one should consider the server specifications as well as storage specifications required for storing session information on targets. Once OPAM has been sized based on the customer's throughput characteristics, then high availability within a single data center and disaster recovery across multiple data centers can be considered. It is important to take into account what the customer's definition of high availability and DR are, as many customers have different approaches. The Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management provides good baseline guidance on this topic.

Oracle Privileged Account Manager Disaster Recovery Architecture

As of the writing of this document, OPAM is officially supported to run in an active/passive configuration for multi site Disaster Recovery (DR). This means that the production instances of OPAM are active, whereas the DR components of OPAM are passive. The passive designation means that the host system will be running but the OPAM WebLogic Instance will not be running during normal operation. Note that OPAM can be configured to run Active/Active within a single datacenter in a high availability configuration, but this paper is focusing on the active/passive configuration for a multi site deployment. Let's take a moment to understand what each component in the architecture is doing during normal operation. There are several key assumptions to understand during this discussion.

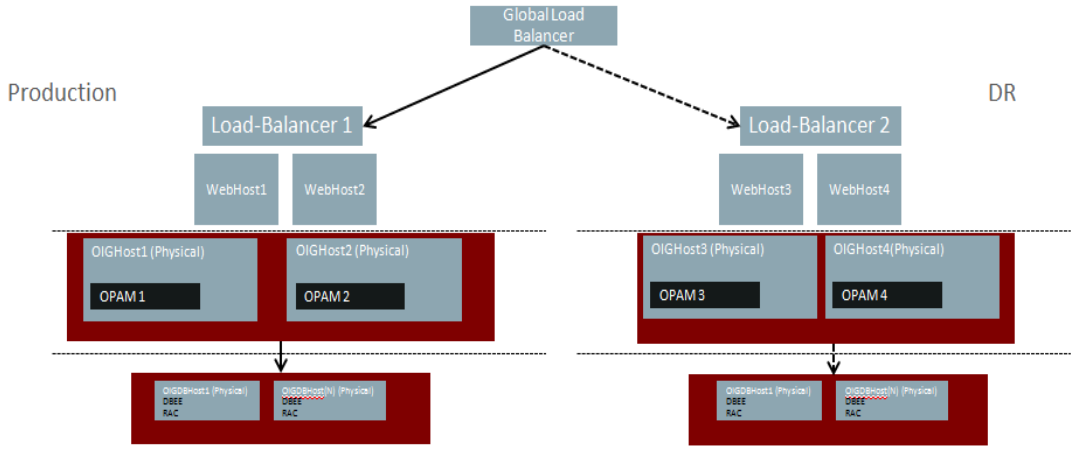

Figure 2: OPAM Prod and Disaster Recovery High Level Architecture

Assumptions:

- The Oracle DB in Production and DR is 2 (or more) instances of RAC.
- Oracle DB comes with Data Guard. Data guard handles the replication of data from the prod DB tier to the DR DB tier during normal operation using a variety of configurations.

- Data Guard can also enable role transition to switch the DR DB from standby to primary during a DR scenario. This can be configured to occur automatically or manually. Active Data Guard is used for a specific purpose outlined in the FAQ section of this paper.
- OPAM3 and OPAM4 are assumed to be preconfigured with appropriate targets and then turned off.
- The WebLogic Server in DR is assumed to be off and OIGHost3 and OIGHost4 are on.
- The WebHosts (1-4), local load balancer, and global load balancer configuration are not in scope for this paper. Customers have many different methods of configuring these components, whether they are using Oracle Http Server, Apache, or another Web server. Similarly, local and global load balancers may be implemented different ways. The Enterprise Deployment guide suggests the recommended method to deploy these components. For the purposes of the paper, we will assume that the customer has the means to route to web tiers as needed.

Normal Operation:

During Normal Operation, the components below will be working as described:

Production Web tier:

This tier may vary depending on the customer. Generally Load Balancer 1 will balance the traffic to the 2 webhost nodes (1 & 2) for HA. If one webhost (webhost1) is unresponsive, Load Balancer 1 routes all traffic to the other webhost (webhost2). The webhost nodes will route the traffic to the OPAM 1 and OPAM 2 instances for HA configuration within the production datacenter.

Production Application Tier:

The application tier will consist of 2 (or more) physical hosts for high availability. Each physical host will be running a WebLogic instance of OPAM. This enables an HA configuration of OPAM in the production datacenter. If one OPAM node (OPAM 1) is unresponsive, webhost1 and webhost2 will need to route the traffic to OPAM 2.

Note: For clients utilizing the OPAM API, an additional Load Balancer in front of OPAM 1 and OPAM 2 can be used to balance API calls between the 2 OPAM instances. Note this traffic is assumed to be internal network traffic. For traffic originating externally, other considerations need to be made.

Note: OPAM1 and OPAM2 WebLogic instances can utilize the high availability built into the Oracle RAC database. The Oracle RAC database can be configured as a JDBC multi data source or GridLink data source to protect the instance from Oracle RAC node failure. GridLink is the recommended method of building in high availability and offers top of the line capabilities for automatic failover. GridLink can be enabled when the “Active Gridlink” feature of WebLogic Suite is licensed (WebLogic Suite is not included in the restricted use license of WebLogic Server Enterprise Edition that comes with the Identity Governance Suite). Active Gridlink allows the WebLogic instances to be “RAC aware” and communicate on the same back channel that the RAC nodes communicate on. This enables the WebLogic server to automatically know when a RAC is down or up and connect to it accordingly without manual intervention. The JDBC multi data source configuration is not as automatic, but can also be used to configure multiple RAC DB connections. JDBC multi data source is used by many customers today.

Production Data Tier:

The production data tier is using Oracle RAC database with 2 or more RAC nodes. This enables quick failover within the production site if there is a RAC node failure. During normal operation, Oracle Data Guard will replicate production data to the DR (standby) RAC database.

Production LDAP:

OPAM relies on and transparently uses the ID Store and Policy Store configured for the WebLogic domain in which OPAM is deployed. All OPAM users and administrators are authenticated using this identity store. It is recommended that customers use a LDAPv3 compliant directory for this purpose. In the production datacenter, the LDAP identity store should be highly available so it can be accessed by the OPAM1 or OPAM2 WebLogic server instances.

DR site during normal operation:

Many customers choose to have a scaled down deployment of OPAM in DR. Depending on the customer's risk analysis, it may be acceptable to have a scaled down DR environment, although the general recommendation is to provide a reliable service even in disaster scenarios. For the purposes of this discussion, we have assumed that the customer has an identical deployment in Production and DR.

DR Web tier:

This tier may vary depending on the customer. It is going to function similar to the production web tier. During normal operation the web tier can be turned on and ready to route traffic or it can be turned off awaiting a call to action.

DR Application Tier:

OPAM supports an Active/Passive deployment for Prod/DR. This means that the WebLogic Server(s) will need to be passive in DR. Assuming the WebLogic tier in DR is connecting to the Oracle DB tier in DR, the DB will be in standby mode until a DB role transition is complete (this is a step in the database failover process). The DR WebLogic Server won't start up properly until the DR DB is made primary. Therefore, during a failover, the DR WebLogic instance needs to be started/restarted in order for the OPAM application to successfully connect to the DR DB (which has transitioned its role to primary). There is some flexibility here depending on the implementation of WebLogic server, for example, scripts can be used to automate some of this process. For the purposes of this discussion, the physical host for the WebLogic Server(s) in DR will be turned on, but WebLogic Server will be off during normal operation.

DR Data Tier:

The DR data tier is using Oracle RAC database with 2 or more RAC nodes. This enables the redundancy and availability benefits of RAC within the DR site. During normal operation, Oracle Data Guard will replicate production data to the DR standby database.

DR LDAP:

OPAM relies on the ID Store and Policy Store configured for the WebLogic domain in which OPAM is deployed. In DR, the LDAP identity store should be highly available so it can be accessed by the OPAM WebLogic server instances. LDAP replication from Prod to DR should be in place so the DR LDAP is available at all times.

Steps Required for Disaster Recovery Failover

Customers want to know what high level steps and credentials are required for a DR failover to occur. Since the current release of OPAM supports an Active/Passive deployment in Production/DR, there will be some manual components to the failover process for the OPAM instance. Furthermore, Data Guard failover steps vary depending on whether Data Broker is used, manual steps are taken, or Fast Start Failover is utilized. For details how Data Guard can be used to failover the Oracle Database see:

https://docs.oracle.com/database/121/nav/portal_14.htm

Oracle Site Guard can automate the failover process for all of a customer's infrastructure components in all tiers. Depending on the complexity of the customer's environment and the number of manual steps that are required, Site Guard may make sense for the customer to automate as much as possible during a failover scenario. Site Guard allows you to extend the built in disaster recovery functionality of Oracle components by allowing you to inset custom scripts at specific points during the operation workflow. It includes the capability to perform pre-checks, health checks, storage integration, monitoring, credential management, and more. Site Guard is not in scope for this paper, but additional information can be found here:

http://docs.oracle.com/cd/E24628_01/server.121/e52894/concepts.htm#GUARD126

The below example gives a simplistic high level overview of the steps required to failover the database. The failure scenario for this discussion assumes that there is a geographic outage and multiple components in multiple tiers in Production are failing. In this scenario, the customer will need to follow some high level steps to failover to the DR OPAM.

High Level Failover Steps Required:

1. The Oracle DB used by OPAM will be failed over to the DR site using one of the methods made available through Data Guard.
2. The WebLogic Server is brought up after the DR DB instance has been transitioned to the primary DB. There are various methods to do this, either manually, using custom scripts, or using Site Guard.
3. The Web Tier components need to be started in the DR Site.
4. Connectivity is confirmed for all DR components. Global traffic needs to be routed to the DR site via a Load Balancer configuration or utilizing Domain Name Services re-configuration.

Note: The steps above will vary greatly depending on the customer environment. For example, the DNS change may be required before anything else to ensure all the components can communicate within the DR site before the global traffic is routed to DR. It is important to understand the steps your customer uses today and provide a general guideline for how OPAM can fit into that process. The implementation partner should be involved in this discussion.

OPAM Credential Storage Considerations

A commonly asked question is: how can OPAM can be started in DR if OPAM's infrastructure credentials are protected by OPAM itself and there is an OPAM outage? OPAM's infrastructure credentials may include the WebLogic administration account required to start WebLogic, the Oracle DBA account to perform DB failover operations, and other accounts that are required to start up and troubleshoot OPAM in the Production and DR environment. This is an interesting chicken and egg scenario, however, it is recommended that all OPAM infrastructure credentials required to start OPAM and all its dependent components are NOT protected by OPAM. The simple reason is you do not want to place the keys to the vault inside the vault. For example, the following credentials should not be stored inside OPAM:

- **DBA account for OPAM DB** – This can be stored in an external password store (Oracle wallet).
- **WLS admin account for starting WLS domains** – This can be encrypted in the boot identity file. The WLS startup script will use those encrypted credentials to start WLS, so the administrator does not need to know the credentials.
- **OS Credentials for OPAM WebLogic Server and DB hosts** – These should be kept outside of OPAM in a secure location.

Note: One method to address this scenario is to use a lower environment (QA/Test) to protect the OPAM infrastructure credentials in Production and to use the Production environment to protect the lower environment's OPAM infrastructure credentials. This gives administrators a way to get the OPAM WebLogic Server, DB, and OS passwords for starting up OPAM in DR, even if OPAM goes down in production. However, it still does not help you during a wide reaching outage that may take down your lower environments in addition to your production environment.

Note: Another option is available for customers that own Oracle Database Vault. This method will limit the number of OPAM infrastructure credentials they need to track and safeguard. . The customer can allow the "oracle" OS account to start up the OPAM DB and the WebLogic Server so no other credentials are required to start up the OPAM infrastructure. This OS user account can start up WLS and the Oracle DB without requiring further authentication. The advantage of this option is that no additional passwords/credentials are required to startup the DR OPAM infrastructure assuming there is no troubleshooting required during the startup of DR. The disadvantage of this option is that it opens up the Oracle DB to individuals that have the "oracle" account credentials. Therefore, it is best practice to use Database Vault to control what commands the "oracle" OS account is allowed to execute on the Oracle DB.

Note: Oracle Site Guard also provides functionality for creating and storing preferred credential associations in a secure manner so the infrastructure credentials required to start up components can be stored in Enterprise Manager.

Oracle Privileged Account Manager Disaster Recovery Scenario FAQ

Does OPAM run in Active/Active multi data center deployment?

No, OPAM supports Active/Passive deployment.

Why Does OPAM only work in Active/Passive Deployment?

The limitation occurs at the WebLogic layer. When you have a primary WLS cluster using a primary DB RAC cluster in normal operation, a DR failover will need to quickly enable all the components in DR starting with the DB, then the WLS tier, then the Web Tier, and finally to route all traffic to DR. Oracle DB uses Data Guard to automatically failover to the standby RAC cluster in DR (and enable a role transition so the standby DB now becomes the primary). At the WLS layer, the production WLS can theoretically point to the standby DR RAC node and failover automatically if the Production RAC nodes are down (Active Gridlink makes this more streamlined). However, if the WLS in production goes down, then in order for the WLS in the DR site to take over, it must be started/restarted in order to connect properly to the DR RAC DB (which was just transitioned to primary). Additionally, there are shared storage components used by the WLS Admin server that must be available. This means that the WLS in DR must be passive, and will not take over operation automatically without scripted or manual intervention.

If OPAM and OIM are integrated as part of an overall Identity Governance Suite solution, what are the interdependencies during a disaster scenario?

In a password vault scenario, Oracle Identity Manager allows the user to "request" access to a privileged account through the OIM catalog. This can kick off a workflow which, once approved, will provision the user into a LDAP group in the OPAM LDAP directory based Identity store and make a password available for the user to login to a target system. OIM disaster recovery is not in scope for this paper, but OIM is technically mutually exclusive from (that is no dependency on) OPAM. OIM will have to be operational for the user to "request" a privileged account, however, as long as OPAM is available the user should be able to "check out" an account password if the account access has already been granted in OPAM. Similarly, OPAM Session Manager is independent of OIM and will be able to govern password or session control for privileged accounts without OIM being operational. In either case the LDAP Identity Store also needs to be HA.

If OPAM is used to store all privileged accounts securely (including accounts needed for the OPAM application), how would administrators get access to start OPAM in DR if production OPAM is down?

It is recommended that minimum credentials to start OPAM in DR are kept outside of OPAM. For example, the credentials to start the OPAM DB can be kept in an Oracle Wallet and the credentials to start WebLogic can be encrypted within a boot script for WebLogic. It is important that these credentials are not kept in the OPAM vault because if there is a production issue, you will not be able to start up the OPAM DR instance without these credentials.

What IT Teams need to be available to start up OPAM in DR?

This really depends on each customer. At a minimum you will need the Oracle DB team to start the OPAM DB. You will need the Oracle WebLogic team to start/restart the WebLogic servers and ensure they are running properly. You will need the Identity and Access Mgmt team to ensure OPAM is running and operational. You will need networking teams to ensure all traffic is being routed properly in DR before a cutover can be made. The exact personnel required, backup individuals required, processes to follow, and phone numbers to call should be practices and documented using a periodic DR exercise to ensure the team is ready.

How should Data Guard be used to make role transition? Automatically or manually?

This depends on the customer preference. Some customers prefer to have as many steps automated as possible, in which case you would automate the role transition. Other customers prefer to start each component individually to ensure it is operational so troubleshooting becomes easier if you run into issues. The pros and cons of each approach need to be weighed by the customer to decide which method makes the most sense based on their DR experience.

Does OPAM support a metro cluster deployment?

A Metro cluster deployment is a deployment where the Production and DR sites are closely meshed together. A Production Application tier will point to the Prod DB tier as primary and the DR tier for backup. Similarly the DR Application Tier will point at the Prod DB tier as primary and the DR tier as backup. In this scenario, if there is a failover in the Data Tier or in the App tier, there is theoretically no manual intervention required for operation to continue (especially if Active Gridlink is used). OPAM does not support a metro cluster deployment as of this writing.

Can an Oracle RAC replicate to a single instance of Oracle DB in DR?

Yes, this can be done and might be considered by the customer if they want the DR DB instance to be minimal.

What is the difference between Data Guard and Active Data Guard?

The main difference between these 2 options is that Active Data Guard gives the customer the ability to READ from a DB that is operating as a standby database. This can be helpful from a performance perspective because all reporting and backend data operations can be run on the standby database instead of the primary database.

Does my infrastructure require any Shared Storage components in order to effectively provide failover capabilities for OPAM?

Shared storage requirements are covered in the Enterprise Deployment Guide. Shared storage comes into play for the configuration of the WebLogic Administration server across multiple instances in a single and multi-data center deployment. There are a number of directories and files that should be stored in shared storage for failover of Administration functionality for WebLogic. Best Practices for shared storage for WebLogic can be found below.

Resources

- Best Practices for Oracle FMW Identity and Access Management (11.1.2.2): Extending an Enterprise Deployment with Oracle Privileged Account Manager

http://www.oracle.com/technetwork/middleware/id-mgmt/overview/edg-opam-111220-wp-2550777.pdf

- Configuring High Availability for Oracle Privileged Account Manager Components

http://docs.oracle.com/cd/E40329_01/doc.1112/e28391/opam.htm

- Oracle WebLogic Server and Highly Available Oracle Databases: Oracle Integrated Maximum Availability Solutions

http://www.oracle.com/technetwork/database/features/availability/wlsdatasourcefordataguard-1534212.pdf

- Oracle Active Data Guard Real-Time Data Protection and Availability

http://www.oracle.com/technetwork/database/availability/active-data-guard-wp-12c-1896127.pdf

- Oracle WebLogic on Shared Storage: Best Practices Whitepaper:

http://www.oracle.com/technetwork/database/availability/maa-fmwsharedstoragebestpractices-402094.pdf

- Oracle Fusion Middleware Disaster Recovery Guide

http://docs.oracle.com/cd/E17904_01/doc.1111/e15250/intro.htm#ASDRG107

- Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager

http://docs.oracle.com/cd/E40329_01/admin.1112/e27152/intro_opam.htm#OPMAG112

- Oracle Site Guard Administrator's Guide

http://docs.oracle.com/cd/E24628_01/server.121/e52894/concepts.htm#GUARD126

- Oracle Database Online Documentation 12c

https://docs.oracle.com/database/121/nav/portal_14.htm

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

ORACLE PRIVILEGED ACCOUNT MANAGER DISASTER RECOVERY DEPLOYMENT CONSIDERATIONS
August 2015
Author: Manny Khadilkar
Contributing Authors: Michael Rhys, Arun Theebaprakasam, Olaf Stullich, David Lee, Advait Deodhar